UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

ALLIANCE FOR AUTOMOTIVE INNOVATION,	)	
Plaintiff,	)	
v.	)	**Civil Action No. 20-12090-DJC**
ANDREA JOY CAMPBELL, ATTORNEY GENERAL OF THE COMMONWEALTH OF MASSACHUSETTS in her official capacity,	)	
Defendant.	)	

CASPER, J. **February 11, 2025**

MEMORANDUM OF DECISION

I. INTRODUCTION

On November 20, 2020, Plaintiff Alliance for Automotive Innovation ("AAI") brought this case against the Attorney General of the Commonwealth of Massachusetts ("the Attorney General") in her official capacity[1] on the heels of the passage of a right-to-repair law by ballot initiative in Massachusetts in the 2020 election ("the Data Access Law"). The Attorney General disputes that AAI has associational standing and each of AAI's claims for conflict preemption with various federal statutes, Counts I through VI, its claims for unconstitutional taking under Count VII and the injunctive relief that it seeks under Count VIII. D. 1. This matter has been

[1] When this action commenced, Maura Healey was serving as the Attorney General. During the pendency of this action, Andrea Joy Campbell succeeded to the office and was automatically substituted as the defendant pursuant to Federal Rule of Civil Procedure 25(d). See D. 329.

awaiting resolution by the Court after a bench trial was concluded in June and July 2021, the reopening of discovery and the Court's solicitation of further briefing in fall 2021 and again in summer 2022 through early winter 2023, D. 282-83, 286, 320, 327, and March 31, 2023, when the Court granted the Attorney General's motion to dismiss as to all of the Counts except Counts I and II (claims for conflict preemption under the National Traffic and Motor Vehicle Safety Act ("MVSA"), 49 U.S.C. § 30101 *et seq.* and the Clean Air Act ("CAA"), 42 U.S.C. § 7401 *et seq.*, respectively), which were the subject of the bench trial. D. 334.[2] This case recently was reassigned to this session of the Court. D. 355 (entered January 7, 2025).

II. PROCEDURAL HISTORY

AAI filed this lawsuit against the Attorney General on November 20, 2020, D. 1, and shortly thereafter, on December 1, 2020, sought a preliminary injunction to prevent the Data Access Law from taking effect. D. 26; D. 27 at 7. On December 18, 2020, the Attorney General moved to dismiss all claims filed against her in this action. D. 75. Based upon the Attorney General's initial stipulation to forego any enforcement of the Data Access Law until a resolution of AAI's claims after an expedited trial, D. 50, AAI conditionally withdrew its motion for preliminary injunction, D. 26, 51, and the Court granted AAI's motion to stay Counts III through VII until after adjudication of Counts I and II. D. 57, 89. The Court denied the Attorney General's motion to dismiss as to Counts I and II under Fed. R. Civ. P. 12(b)(1) and 12(b)(6), D. 75, 93, but stayed any discovery as to the other claims, making clear that the denial of the motion as to associational standing was without prejudice, noting that standing is "almost coincidental with the merits" to be considered at the expedited trial on Counts I and II. D. 93; D. 94 at 7-8. The Court

[2] This Order also denied the Attorney General's motion for judgment as a matter of law, D. 204, filed on the first day of the bench trial. D. 334.

also expressed some concern about whether hypothetical risk is sufficient for AAI to show conflict preemption and expressed some skepticism about whether, for example, mere guidance from the National Highway Traffic Safety Administration ("NHTSA") about cybersecurity was sufficient to show such conflict, but denied the motion to dismiss without prejudice as to Counts I and II. D. 94 at 9-10, 13-14, 17-19, 24-25, 44-45.

After a course of fact and expert discovery, a series of motions to compel, D. 101, 120, conferences and multiple pretrial conferences, see, e.g., D. 134, 139, 149, 166, 193, 195, the Court conducted a bench trial that began on June 14, 2021, approximately seven months after AAI filed its lawsuit.[3] The five-day trial went forward with AAI's fact witnesses (representatives from AAI and from two of AAI's car manufacturer members, General Motors Company ("GM") and FCA US LLC ("FCA" or "Fiat")) and two experts, and two fact witnesses and two experts introduced by the Attorney General.[4]

Following trial, the discovery record was reopened, and the Court solicited additional briefing on various issues. In October 2021, the Attorney General filed a motion to reopen the trial evidence to supplement with facts concerning the actions of one car manufacturer with respect

[3] Although the United States filed a statement of interest shortly prior to trial expressing concerns about the impact of the Data Access Law as to cybersecurity risk and the timing requirement of the new law, it took no position at that time about whether the Data Access Law was preempted by the MVSA, the CAA or any of the other federal statutes identified in AAI's claims. D. 202 at 3, 6 n.7, 8-9.

[4] The Court will discuss this issue further in its analysis of the associational standing issue, but GM, Fiat and other car manufacturers are members of AAI, but not parties to this litigation. Although AAI initially planned to offer testimony from four car manufacturers, GM, Fiat, Mercedes-Benz USA, LLC ("MBUSA") and Toyota Motor North America, Inc. ("Toyota"), see D. 112 at 7-8; D. 134 at 20, their participation in discovery was only "voluntary," D. 112 at 19, and after the Court suggested that if the latter entities did not make the document production sought by the Attorney General in her motion to compel, it might strike their affidavits as to associational standing, D. 134 at 21, AAI removed Toyota and MBUSA representatives as witnesses. D. 139 at 19-20.

to its telematics system, D. 245, which the Court granted, D. 253. Also in October 2021, the Court solicited briefing on issues raised by the United States as *amicus curiae* in Volkswagen Grp. of Am., Inc. v. Env't Prot. Comm'n of Hillsborough Cnty., No. 20-994 (2021). D. 254 at 5. In September 2022, the Court solicited briefing regarding the parties' respective textual interpretations of the Data Access Law and the steps taken by the parties to implement the requirements of the Data Access Law. D. 279, 282, 283, 286. In November 2022, AAI requested additional discovery from the Auto Care Association, a proponent of the Data Access Law, that had also become a proponent of a proposed Maine right-to-repair ballot initiative. D. 307, 318; see D. 320, 327. In March 2023, the Court ordered briefing regarding testimony by an Auto Care Association representative and the additional documents produced by the Auto Care Association with respect to the Data Access Law and enforcement thereof. D. 333.

On March 7, 2023, the Attorney General filed a notice of intent to terminate, effective June 1, 2023, the non-enforcement stipulation previously entered in this action by which the Attorney General had agreed to delay engaging in any action pursuant to her notice and enforcement authority as provided for by the Data Access Law. D. 330. On March 31, 2023, the Court issued an order granting the Attorney General's motion to dismiss as to Counts III through VIII. D. 334. On May 25, 2023, AAI filed an emergency motion for a temporary restraining order, D. 339, which the Court denied without prejudice to a request for a preliminary injunction, D. 345; D. 343 at 16-17. At the May 30, 2023 hearing on the motion for a temporary restraining order, counsel for the Attorney General represented that penalty provisions under the Data Access Law would not retroactively be imposed, and the parties agreed to advise the Court of any litigation commenced after June 1, 2023. D. 343 at 8-10; D. 345.

The Court takes judicial notice that on June 1, 2023, the Attorney General published the Massachusetts Vehicle Telematics System Notice pursuant to Section 4 of the Data Access Law, codified at Mass. Gen. L. c. 93K, § 2(g).[5]

On June 13, 2023, the United States notified the Court and the parties that NHTSA had transmitted a letter that same day to motor vehicle manufacturers expressing its view that "the Data Access Law conflicts with and therefore is preempted by the [MVSA]." D. 346; D. 346-1 at 2 ("June 2023 NHTSA Letter"). The letter stated, among other things, that "[g]iven the serious safety risks posed by the Data Access Law, taking action to open remote access to vehicles' telematics units in accordance with that law, which requires communication pathways to vehicle control systems, would conflict with . . . the [MVSA]," D. 346-1 at 3, and that "[b]ecause the [MVSA] conflicts with and therefore preempts the Data Access Law, NHTSA expects vehicle manufacturers to fully comply with their Federal safety obligations," id. at 4.

On August 22, 2023, the United States notified the Court and the parties that on that day, NHTSA transmitted a letter to the Attorney General in which it stated that NHTSA was "pleased to have worked with [the Attorney General] to identify a way that the Massachusetts Data Access Law may be successfully implemented—promoting consumers' ability to choose independent or do-it-yourself repairs—without compromising safety." D. 351; D. 351-1 at 1 ("August 2023 NHTSA Letter"). Among other things, the August 2023 NHTSA Letter stated that "NHTSA understands that, according to the Massachusetts Attorney General, one way that vehicle manufacturers can comply with the Data Access Law is by providing independent repair facilities wireless access to a vehicle from within close physical proximity to the vehicle, without providing

[5] See Massachusetts Vehicle Telematics System Notice, https://www.mass.gov/doc/2023-6-1-telematics-right-to-repair-notice/download (last accessed February 6, 2025).

long-range remote access." D. 351-1 at 1. It further expressed NHTSA's view that "[s]uch a short-range wireless compliance approach, implemented appropriately, . . . would not be preempted," id., and acknowledged the "common understanding" of the Attorney General and NHTSA "that implementing this compliance option with the secure 'open access platform,' as required in the [Data Access] Law, is not immediately available, and that vehicle manufacturers may require a reasonable period of time to securely develop, test, and implement this technology," id. at 2. Also on August 22, 2023, the Attorney General notified the Court that it had transmitted a letter to NHTSA in response to the August 2023 NHTSA Letter. D. 352. Among other things, the Attorney General "confirm[ed] NHTSA's understanding that a platform that provides the required features, capabilities, and access using a short-range wireless protocol such as Bluetooth is one approach that a vehicle manufacturer might use to achieve compliance with the Data Access Law." D. 352-1 at 2. On September 22, 2023, AAI filed a response to the notices filed by the Attorney General and the United States. D. 353. AAI noted that its "members are unable to properly assess the feasibility of the approach that the Attorney General and NHTSA have proposed," id. at 3, but that it "look[ed] forward to working with NHTSA and the Attorney General to discuss in more detail a potential future compliance methodology that would not be preempted by federal law," and that "[i]n the meantime, [AAI] and its members intend to continue to abide by NHTSA's instruction in [the June 2023 NHTSA Letter]." Id. at 4; see id. at 3.

On January 7, 2025, the case was reassigned to this session of the Court (Casper, J.). D. 355. The same day, the undersigned judge advised the parties that she had reviewed the record in this case, including the transcripts of the bench trial conducted in June and July 2021 and the pre-trial and post-trial filings, and thereby certified familiarity with the record and, accordingly, that the case may be completed by this session without prejudice to the parties pursuant to Fed. R.

Civ. P. 63. D. 356. Having concluded that no further briefing on the merits of the issues was necessary given the trial record and extensive briefing, the Court gave the parties leave to file any motion to recall witnesses under Rule 63 and/or file a status update, by January 17, 2025. Id. AAI filed such motion by the deadline seeking to recall three of its witnesses and call an additional witness, D. 357, which the Attorney General opposed. D. 358 at 8; D. 360. The Court denied AAI's motion to recall witnesses but gave counsel for both parties an additional opportunity for final arguments on the completed record before this session of the Court and scheduled same for February 4, 2025. D. 361, 362. On February 4, 2025, the Court heard final arguments from counsel. D. 363, 364.

III. FINDINGS OF FACT

Based upon the record developed at trial, and pursuant to Fed. R. Civ. P. 63 where the undersigned certifies her familiarity with the record and having determined that the case can be completed in this manner without prejudice to the parties given the full presentation of their claims, defenses and arguments at trial and otherwise during the course of this case and that the recall of the three witnesses that AAI sought to recall (and the additional witness it sought to add) is not warranted, see D. 361 (explaining reasons for denial of AAI's motion filed pursuant to Rule 63), the Court makes the following findings of facts and conclusions of law as to associational standing and Counts I and II, ruling in favor of the Attorney General as to these remaining claims.

A. The Parties

1. Plaintiff AAI is a trade association comprising auto manufacturers, also known in the industry as original equipment manufacturers ("OEMs"). AAI's membership includes most, but

not all, OEMs that currently manufacture automobiles for sale in the United States. D. 235 ¶ 1; D. 236 ¶ 1.[6]

2. Defendant Andrea Joy Campbell is sued in her official capacity as Attorney General of Massachusetts. As Attorney General, she has authority to enforce the Data Access Law. D. 236 ¶ 98.

B. The Data Access Law

3. In 2012, the Auto Care Association and other "aftermarket" trade organizations collected sufficient signatures to place a "right to repair" ballot question on the ballot for Massachusetts voters. D. 235 ¶ 39.[7]

4. Massachusetts voters overwhelmingly approved the ballot question, by a margin of 86%, D. 200 at 60, and it became law in 2013 and is now codified at Mass. Gen. L. c. 93K; D. 235 ¶ 40; D. 236 ¶ 100. See Massachusetts Elections Statistics 2012, Secretary of the Commonwealth of Massachusetts, Public Document No. 43 at 534-35,

[6] Prior to final arguments in the bench trial, D. 239, the parties filed revised, proposed findings of fact and conclusions of law, D. 232, 233, and were also given the opportunity to "mark up" the proposed findings and conclusions by the opposing party, D. 235, 236; see D. 234 at 1. To the extent possible, the Court has referenced the latter filings, D. 235, 236, in this Memorandum of Decision.

[7] Generally, "aftermarket" refers to everything that happens to a motor vehicle after it leaves the showroom. D. 235 ¶ 32; D. 191 ¶ 1. "Independent aftermarket" refers to aftermarket businesses, such as independent repair shops, that are not affiliated with an OEM. D. 235 ¶ 34; D. 191 ¶ 2. The "right to repair" title for the 2012 and 2020 ballot initiatives reflects the position of the aftermarket trade associations and the Attorney General that independent repair shops can be a less expensive option for consumers to get service and repairs to their motor vehicles and that as vehicles have become more technically sophisticated and access to technical and diagnostic information is necessary for repairs, independent repair shops can be at a disadvantage in comparison to the OEM dealerships in offering such service and repairs to consumers. See D. 235 ¶¶ 32, 37-38; D. 191 ¶¶ 8-12.

https://electionstats.state.ma.us/data/serve_file_pages_for_item/6811/BallotQuestion/; 2013 Mass. Legis. Serv. Ch. 165 (H.B. 3757) (West).

5. After the enactment of the 2013 law, an alliance of aftermarket trade associations, the Alliance of Automobile Manufacturers and the Association of Global Automakers entered into a Memorandum of Understanding ("MOU") in January 2014 that extended the Massachusetts 2013 law requirements nationally. D. 191 ¶ 44; D. 235 ¶ 41; D. 236 ¶ 101.

6. At the time of the 2013 law and the MOU, telematics was a new technology. D. 191 ¶ 49; D. 235 ¶ 41.

7. The 2013 law largely excluded telematics, see Mass. Gen. L. c. 93K, § 2(f) (providing that "[w]ith the exception of telematics diagnostic and repair information that is provided to dealers, necessary to diagnose and repair a customer's vehicle and not otherwise available to an independent repair facility . . . nothing in this chapter shall apply to telematics services or any other remote or information service, diagnostic or otherwise, delivered to or derived from a motor vehicle by mobile communications") (Nov. 26, 2013), as did the MOU. D. 191 ¶ 49.

8. Although the parties dispute the exact impetus for the subsequent 2020 Right to Repair ballot initiative, the Attorney General contends that there were some OEM compliance issues with the 2013 law and that the rise of the use of telematics by OEMs also contributed to the second ballot initiative. D. 235 ¶¶ 42-49; D. 191 ¶¶ 51-60.

9. Telematics systems on motor vehicles provided the OEM with the capability of transmitting mechanical data for diagnosis, repair and maintenance wirelessly. D. 235 ¶ 44.

10. The Attorney General contends that these telematics systems made it easier for OEMs to access such data on motor vehicles, but more difficult for independent repair shops to do so. D. 235 ¶¶ 45-46; D. 191 ¶¶ 61-67.

11. Starting in or around 2016, the Auto Care Association began making technical presentations to AAI and others, including individual OEMs, about a method to provide independent repair shops access to telematics system data. D. 235 ¶ 47; D. 191 ¶¶ 68-81.

12. At some point after these efforts, a coalition including the Auto Care Association and others gathered sufficient signatures to have Ballot Question 1, regarding the Right to Repair, on the 2020 ballot. D. 191 ¶¶ 83-85; D. 235 ¶¶ 49-50; Signed Initiative Petition regarding An Initiative Law to Enhance, Update and Protect the 2013 Motor Vehicle Right to Repair Law, https://www.mass.gov/doc/19-06-initiative-law-to-enhance-update-and-protect-the-2013-motor-vehicle-right-to-repair-law/download (last accessed February 7, 2025).

13. The proposed law, as summarized for voters on the ballot, "would require that motor vehicle owners and independent repair facilities be provided with expanded access to mechanical data related to vehicle maintenance and repair." Secretary of the Commonwealth of Massachusetts, Election Results Archive, 2020 Statewide Question 1, https://electionstats.state.ma.us/ballot_questions/view/7343/ (last accessed February 7, 2025). The summary on the ballot further explained that "[s]tarting with model year 2022, the proposed law would require manufacturers of motor vehicles sold in Massachusetts to equip any such vehicles that use telematics systems . . . with a standardized open access data platform," and that "manufacturers would not be allowed to require authorization before owners or repair facilities could access mechanical data stored in a motor vehicle's on-board diagnostic system, except through an authorization process standardized across all makes and models and administered by an entity unaffiliated with the manufacturer." Id.

14. On November 3, 2020, Massachusetts voters overwhelmingly approved Ballot Question 1, D. 235 ¶ 53; D. 236 ¶ 97, by a margin of 75%. D. 275-1 at 4; D. 191 ¶ 88; Secretary of the

Commonwealth of Massachusetts, Election Results Archive, 2020 Statewide Question 1, https://electionstats.state.ma.us/ballot_questions/view/7343/ (last accessed February 7, 2025).

15. That law, referred to hereinafter as the "Data Access Law," became effective in December 2020. D. 236 ¶ 97; D. 235 ¶ 54.

16. The Data Access Law amended Mass. Gen. L. c. 93K, which was previously enacted in 2013. See D. 235 ¶¶ 39-40; D. 236 ¶ 100.

17. The key provisions of the Data Access Law at issue in this case are Section 2 and Section 3. See D. 235 ¶¶ 58-74; D. 236 ¶¶ 107-20 (describing AAI's view of "Effect of Section 2"); id. ¶¶ 121-52 (describing AAI's view of "Effect of Section 3").

18. The Data Access Law also amended chapter 93K to add two new definitions, for "mechanical data" and for "telematics system." D. 235 ¶ 55.

19. Chapter 93K, as amended, defines "mechanical data" as "any vehicle-specific data, including telematics system data, generated, stored in or transmitted by a motor vehicle used for or otherwise related to the diagnosis, repair or maintenance of the vehicle." D. 235 ¶ 56; Mass. Gen. L. c. 93K, § 1.

20. Chapter 93K, as amended, defines "telematics system" as "any system in a motor vehicle that collects information generated by the operation of the vehicle and transmits such information, in this chapter referred to as 'telematics system data,' utilizing wireless communications to a remote receiving point where it is stored." D. 235 ¶ 57; Mass. Gen. L. c. 93K, § 1.

21. Section 2 of the Data Access Law is codified at Mass. Gen. L. c. 93K, § 2(d)(1). D. 235 ¶ 58; 236 ¶ 107. It adds to the statute that "motor vehicle owners' and independent repair facilities' access to vehicle on-board diagnostic systems shall be standardized and not require any authorization by the manufacturer, directly or indirectly, unless the authorization system for access

to vehicle networks and their on-board diagnostic systems is standardized across all makes and models sold in the Commonwealth and is administered by an entity unaffiliated with a manufacturer." Mass. Gen. L. c. 93K, § 2(d)(1).

22. Section 3 of the Data Access Law amends Mass. Gen. Laws c. 93K, § 2, by replacing subparagraph (f), which exempted certain telematics data, with a new subparagraph (f). D. 235 ¶ 63.

23. Section 3 of the Data Access Law is codified at Mass. Gen. L. c. 93K, § 2(f). D. 236 ¶ 121. It provides, in relevant part, that "[c]ommencing in model year 2022," "a manufacturer of motor vehicles sold in the Commonwealth . . . that utilizes a telematics system shall be required to equip such vehicles with an inter-operable, standardized and open access platform across all of the manufacturer's makes and models." Mass. Gen. L. c. 93K, § 2(f).

24. The Data Access Law does not prescribe a specific method of compliance with these provisions. D. 235 ¶ 171.

C. Manufacture of Automobiles by AAI Members

25. One member of AAI is GM. D. 196 ¶ 2; D. 197 ¶ 4; D. 235 ¶ 2. GM is a manufacturer of automobiles sold in the United States, and specifically in Massachusetts, that bear nameplates including Chevrolet, Cadillac, GMC and Buick. D. 235 ¶ 2; see D. 236 ¶ 3.

26. Another member of AAI is Fiat. D. 196 ¶ 2. Fiat is a manufacturer of automobiles sold in the United States, and specifically in Massachusetts, that bear nameplates including Dodge, Chrysler and Fiat. D. 235 ¶ 3; D. 236 ¶¶ 2, 4.

27. AAI offered the testimony of representatives of GM and Fiat during the trial in this case.

28. Another member of AAI is Toyota. D. 196 ¶ 2. Although AAI initially offered Toyota as a "representative" manufacturer, it withdrew its participation in discovery and it was not one of the members offered by AAI during the trial. See D. 235 ¶¶ 5-6.

29. Another member of AAI is Subaru of America ("Subaru").[8] D. 262 (joint stipulation); D. 196 ¶ 2. Subaru is not one of the OEMs that AAI proffered to give testimony during the bench trial in this case.

D. Compliance with the Data Access Law

30. As to Counts I and II, AAI asserts conflict preemption, contending that OEMs cannot comply with the Data Access Law and the dictates of the federal MVSA (Count I) or the CAA (Count II). The Attorney General disputes this contention.

31. Much of this dispute centers around the parties' different interpretations of the Data Access Law, which this Court addresses below.

32. During the bench trial, the parties presented evidence regarding potential compliance with the Data Access Law.

33. Over the course of three days of evidence, six fact witnesses and four expert witnesses were presented by the parties.

[8] In October 2021, after the conclusion of trial, the Attorney General moved to reopen the trial evidence to supplement the record with newly discovered evidence concerning Subaru's making its model year 2022 vehicles ineligible for Subaru's "STARLINK" telematics system if the vehicle is associated with a Massachusetts address. D. 245. The Attorney General contended that this discovery bore on one of the "principal dispute[s]" at trial, about the ability of OEMs to comply with the Data Access Law and with federal law. Id. at 1-2. AAI opposed the motion, D. 250, which the Court granted. D. 253, 254. On November 3, 2021, the parties each filed a status report notifying the Court that they were working toward a stipulation of additional facts that would address the Subaru-related issues, D. 258, 259, and on November 26, 2021, the parties filed their joint stipulation. D. 262.

34. AAI called (i) Steven Douglas, Vice President of Energy and Environment for AAI, D. 196 (amended affidavit),[9] D. 219 at 9-34; (ii) Kevin Tierney, Vice President of Global Cybersecurity at GM, D. 197 (amended affidavit), D. 219 at 35-92; (iii) Kevin Baltes, Director of Product Cybersecurity at GM, D. 198 (amended affidavit), D. 219 at 95-120; (iv) Mark Michael Chernoby, Chief Technical Compliance Officer at FCA, D. 199 (amended affidavit), D. 219 at 120-59; (v) Bryson Bort, AAI's expert, D. 200 (amended affidavit), D. 219 at 162-239; and (vi) Daniel Garrie, AAI's expert, D. 201 (amended affidavit), D. 219 at 240-68.

35. The Attorney General called (i) Aaron Lowe, Senior Vice President of Regulatory and Government Affairs at the Auto Care Association, D. 191 (amended affidavit), D. 220 at 12-90; (ii) Gregory Potter, Chief Technology Officer at the Equipment and Tool Institute ("ETI"), a trade association of automotive tool and equipment manufacturers and technical information providers, D. 161-2 (affidavit), D. 220 at 90-111; (iii) Craig Smith, the Attorney General's expert, D. 192 (amended affidavit), D. 220 at 111-73; and (iv) Brian Romansky, the Attorney General's expert, D. 161-4 (affidavit), D. 220 at 174-237.

36. Much of the testimony of AAI's witnesses was about vehicle architecture, the steps taken to ensure cybersecurity for vehicles and concerns about compliance with the Data Access Law.

37. As Bort testified, "[m]odern vehicles contain complex vehicle architectures, comprising various electronic control units ('ECUs'), sensors, and other electronic components." D. 200 ¶ 18; see D. 201 ¶ 20 (Garrie's diagram illustrating same); D. 192 ¶¶ 28-47 (Smith's attesting about architecture components).

[9] As this Court has previously explained, D. 361, the bulk of testimony proffered at trial was by affidavit. Id. As directed by the Court, direct examination was by affidavit, subject to cross examination, redirect examination and recross examination. Accordingly, the references here are to the witnesses' affidavits and the transcript of their testimony at trial.

38. There is no one structure of vehicle architecture across OEMs, D. 200 ¶ 18, and it can vary across make, model and year, D. 192 ¶ 22, but OEMS have adopted common approaches to same. D. 200 ¶ 18.

39. For one example, in terms of differences in such architecture, the number, scope and layout of ECUs in a vehicle can vary as can the capacities of same. D. 192 ¶¶ 28, 32.

40. ECUs are connected to each other by a network, most commonly by a CAN bus network. D. 192 ¶¶ 37-40.

41. For CAN-based networks, diagnostic communications occur through Unified Diagnostic Services ("UDS"). D. 192 ¶ 46.

42. UDS is what diagnostic scan tools (devices that connect to a vehicle through the OBD-II connector, referenced below, to perform diagnostic functions) primarily use for communications to a vehicle's different ECUs. Id.

43. Standardized access to vehicle data for independent repair shops has been required for emissions data for some time.

44. Since the 1990s, the Environmental Protection Agency ("EPA") requires an on-board diagnostic ("OBD") system, now called the OBD-II, to monitor emissions systems. D. 191 ¶¶ 20-23 (citing 42 U.S.C. § 7521(m)(5); 40 C.F.R. § 86.1808-01(f)(2)(i); 40 C.F.R. § 86.010-38(j)(3)(i)); D. 161-2 ¶¶ 12-14; D. 219 at 22; D. 197 ¶ 39.

45. No manufacturer authorization is needed to access many OBD diagnostic codes. D. 197 ¶ 39; see D. 199 ¶¶ 8, 36.

46. The OBD-II port (also known as the J-1962 connector) "offers a standard way for vehicle manufacturers to interoperate with independent repair shops and dealers for emissions and non-emissions diagnostics." D. 201 ¶ 31; D. 192 ¶ 48; D. 219 at 22.

47. The OBD-II port need not only be used for emissions data as required by the EPA, as it has become an access point for conveying other diagnostic, maintenance and repair data using a scan tool. D. 192 ¶ 51; D. 161-2 ¶ 14.

48. The GM witnesses (Tierney and Baltes) discussed the layered measures of protection that GM has taken as to cybersecurity (i.e., "a defense-in-depth approach") to keep its vehicles "in safe condition, avoid unreasonable safety risks, and avoid recalls." D. 197 ¶¶ 20, 40-42; see D. 198 ¶¶ 6-25; D. 219 at 72. AAI's experts, Bort and Garrie, discussed this approach as well. D. 200 ¶¶ 26-49; D. 201 ¶¶ 43-63.

49. Similarly, Chernoby of Fiat explained that Fiat's cybersecurity controls for its vehicles are "highly interdependent and multi-layered." D. 199 ¶¶ 45-55.

50. Tierney of GM attested that such is done "consistent with NHTSA best practices and manufacturers' federal regulatory obligations," D. 197 ¶ 20, including in regard to the CAA's prohibition against removing design elements installed to comply with EPA emissions requirements. Id. ¶ 28.

51. The "defense-in-depth" approach to cybersecurity, however, does not prescribe the specific ways in which layers of protection are built or structured to provide cybersecurity and there can be multiple ways to approach same. D. 219 at 253; id. at 194.

52. Both Tierney of GM and Chernoby of Fiat testified that the requirements of Sections 2 and 3 of the Data Access Law run counter to the cybersecurity approaches of GM and Fiat, respectively, and neither was aware of any currently existing system architecture that would meet the requirements of same. D. 197 ¶¶ 85-91, 99; D. 199 ¶¶ 64-65, 78-79. Garrie expressed a similar opinion. D. 201 ¶ 120.

53. Both Tierney of GM and Chernoby of Fiat testified about the long lead time that their manufacturers would need, as of 2021, to comply with the requirements of the Data Access Law. D. 197 ¶ 12; D. 199 ¶¶ 5-6; see D. 200 ¶¶ 91-92; see also D. 201 ¶¶ 108, 123.

54. These witnesses and AAI's experts, Bort and Garrie, testified about safety and security concerns if OEMs had to remove safety and emissions systems built into their systems, D. 200 ¶ 50; D. 201 ¶¶ 70-71, 89, and if authorization and authentication did not remain with OEMs. D. 200 ¶ 53.

i. ***Compliance with Section 2***

55. Possible means of compliance with Section 2 proffered by the Attorney General were based, at least in part, upon discovery from GM and Fiat, only two members of AAI. See D. 192 ¶¶ 30-32, 54, 62-63, 76-79, 82-83, 85, 99, 109, 132, 138-39, 152-53, 191, 208.

56. Accordingly, the means by which OEMs may fully comply with Section 2 might vary.

57. Some OEMs, but not GM or FCA, allow access to their on-board diagnostic systems without requiring any manufacturer authorization. D. 235 ¶ 172.

58. That is, some OEMs, but not GM, use an on-board diagnostics system in a manner that does not depend on the OEM for authorization. Such OEMs work through ETI (a trade association of automotive tool and equipment manufacturers and technical information providers) to allow independent repair shops to use a scan tool to access the vehicle's on-board diagnostics system without seeking or obtaining authorization from the OEM. D. 235 ¶ 173; D. 161-2 ¶¶ 27-31.

59. Moreover, there is technology available that would allow compliance with Section 2's requirement that a motor vehicle owner and independent repair shop's access to a vehicle's on-board diagnostics system be standardized and not require authorization by the OEM. One such method would be the use of public key infrastructure ("PKI") technology and authentication

techniques that authorize the requisite level of access necessary for independent repair shops to diagnose and make all necessary repairs. D. 235 ¶ 177; D. 161-4 ¶¶ 42-44.

60. The use of PKI technology could replace manufacturer authorization (which is presently the entity that authorizes same for some vehicles) to access on-board diagnostics systems with a secure authorization system administered by an entity unaffiliated with an OEM. D. 161-4 ¶ 6; see D. 219 at 101.

61. Administration of PKI systems by unaffiliated entities is common and well established in other industries, such as internet web browsers. D. 161-4 ¶¶ 22-27.

62. Another method of compliance with Section 2 might be to build on the V2X security solution that has been developed by some OEMs in collaboration with the U.S. Department of Transportation ("DOT") and other global regulatory bodies. D. 235 ¶ 185; D. 161-4 ¶¶ 33-41.

63. V2X refers to secure wireless connections between vehicles and any external services. Originally developed for fast Vehicle-to-Vehicle ("V2V") messaging to support collision avoidance, this technology has been extended and validated for use in Vehicle-to-Infrastructure ("V2I") (secure wireless connections between vehicles and roadside equipment) and broader Vehicle-to-Anything ("V2X") messaging. D. 235 ¶ 186.

64. The V2X capability is powered by a new type of certificate authority infrastructure called the Security Credential Management System ("SCMS"), which is currently supported by the DOT. Id. ¶ 190. Even if SCMS has not been implemented on a large scale, see D. 219 at 232, this infrastructure and authentication capability can be extended to support advanced authentication for vehicle diagnostics and repair. D. 235 ¶ 190.

65. That Section 2 requires an authorization system administered by an entity unaffiliated with any OEM, Mass. Gen. L. c. 93K, § 2(d)(1), does not mean that OEMs would not be involved in development of such entity. See D. 235 ¶ 192.

66. There are past examples of cooperative efforts to create such programs, such as the OEMs' involvement in the creation of the Secure Data Release Model ("SDRM"), a voluntary program developed by OEMs, new car dealers, independent repair shops and locksmiths, which is administered by the National Automotive Service Task Force ("NASTF"). D. 235 ¶ 195; D. 196 ¶¶ 16-24 (explaining SDRM program); D. 219 at 10-16, 26-27; D. 220 at 42-43, 77-78.

ii. ***Compliance with Section 3***

67. Possible means of compliance with Section 3 proffered by the Attorney General were based, at least in part, upon discovery from GM and Fiat, only two members of AAI. See D. 192 ¶¶ 30-32, 54, 62-63, 76-77, 82-83, 85, 99, 109, 132, 138-40, 152-53, 191, 208.

68. A vehicle that is not equipped with a telematics system is not subject to the requirement in Section 3 of the Data Access Law that the vehicle be equipped with an "inter-operable, standardized and open access platform." Mass. Gen. L. c. 93K, § 2(f); D. 235 ¶ 198; see D. 236 ¶ 126.

69. Accordingly, if a vehicle does not have a telematics system or has such disabled, it is not subject to the requirements of Section 3.

70. Such disabling of telematics would be one way of complying with Section 3 or, more accurately, avoiding the necessity of complying with Section 3.

71. Not all OEMs use telematics. D. 235 ¶ 199.

72. Fiat and GM both manufacture vehicles with telematics. D. 30 ¶ 11; D. 197 ¶ 6.

73. Fiat and GM each permit a customer to opt out of functioning telematics services when purchasing a new vehicle. D. 235 ¶ 202.

74. Not all GM vehicles are equipped with its telematics system, the OnStar system. D. 235 ¶ 84; see D. 197 ¶ 6, but most of its consumer vehicles are so equipped. D. 197 ¶ 111; D. 198 ¶ 4. A customer may order a vehicle without such telematics and, however desirable or not it might be, D. 197 ¶ 111; D. 201 ¶¶ 98-106; D. 192 ¶¶ 102-04 (discussing some of the customer features that would be lost if telematics systems were disabled), such telematics system may be disabled at the customer's request or by GM. D. 235 ¶ 91; D. 219 at 57-58.

75. Some Fiat vehicles have telematics systems. D. 219 at 122.

76. Remote, over-the-air updates to vehicles would not be possible in the absence of telematics, but as was true before the recent advent of telematics, such updates could be done physically in the vehicle. D. 192 ¶ 106.

77. Like Fiat and GM, Subaru is also a member of AAI, D. 262 ¶ 1, even as Subaru of New England ("SNE"), an independent company with the wholesale distributorship rights for Subaru vehicles throughout New England, is not an AAI member. Id.

78. Subaru sells model year 2022 vehicles to SNE, which in turn distributes those vehicles to independently owned and operated Subaru dealerships in New England. Id.

79. Certain of Subaru's model year 2022 vehicles are able to use its telematics system, the STARLINK Safety and Security system. Id. ¶ 2.

80. As a result of Section 3 of the Data Access Law, Subaru decided not to make its telematics system available to Massachusetts residents who purchase or lease model year 2022 vehicles. Id. ¶ 3.

81. There is no suggestion in the record that the choice to comply with Section 3 in this way by reverting to a pre-telematics system is unsafe. See D. 219 at 241-42 (acknowledging by Garrie that the features that would be turned off by disabling telematics would not make the vehicle unsafe); D. 219 at 76, 90 (noting by Tierney that even "without telematics GM vehicles are safe").

82. Kia Motors America, Inc. ("Kia") is a member of AAI. D. 44 ¶ 1; D. 47 ¶ 1.

83. "As a result of the Data Access Law, Kia has made its telematics services, which are currently called Kia Connect and formerly called UVO link, unavailable on Model Year 2022 and newer vehicles that are purchased or sold in Massachusetts." D. 263-1 at 9. "This policy became part of the Kia Connect (then known as UVO) Terms of Service published in February 2021, shortly before the first Model Year 2022 Kia vehicles were being offered for sale by dealers." Id. at 10.

84. Another alternative for an OEM to comply with Section 3 would be to equip its vehicles with a platform that builds off of the already existing J-1962 connector. D. 235 ¶¶ 208-09; D. 192 ¶¶ 120-21.

85. Such compliance would utilize a telematic "dongle" (i.e., a device that plugs into a vehicle to provide additional functionality) plugged into the J-1962 port. D. 235 ¶¶ 208, 212; D. 192 ¶¶ 122-23.

86. Existing dongles can send and receive information through J-1962 connectors without manufacturer authorization so long as no gateway within the vehicle blocks the transmission of such information. D. 235 ¶ 214.

87. A dongle with telematic or wireless capabilities can enable a vehicle owner to use a mobile device to send and receive all mechanical data via the J-1962 connector. Id. ¶ 212.

88. Access to such dongles could be granted to vehicle owners who could grant additional keys to an independent repair shop and the repair shop could have a tool that requires the vehicle owner to validate ownership for usage on the vehicle. Id. ¶ 216; D. 192 ¶¶ 132-36.

89. Regardless of whether a vehicle has a secure gateway (i.e., a gateway that has extra security features like filtering and blocking of certain network traffic, D. 220 at 131-32),[10] there are other security measures, such as ECU authentication and message authentication that could remain in place in OEMs using the J-1962 connector as the platform provided that such authorization was administered by an entity unaffiliated with an OEM as required under Section 2. D. 235 ¶ 219; D. 192 ¶¶ 132-36, 141-62.

90. This means of potential compliance with Section 3 would take more time to develop than the immediate approach of disabling telematics, D. 192 ¶ 121; D. 221 at 102-04, but would build off of the use of the OBD-II, J-1962, that is already required in emissions-producing vehicles for access to emissions data by independent repair shops.

91. A third means of compliance with Section 3 would be a fully telematic diagnostic platform in a vehicle. D. 235 ¶¶ 208, 222-32; D. 192 ¶¶ 173-210.

92. Such a telematic platform would consist of an independent module or wireless capabilities embedded in the vehicle's system that would utilize wireless communications. D. 235 ¶ 222; D. 192 ¶¶ 173-75.

93. Given the wireless nature of same, a fully telematic platform should be segmented and isolated from the majority of the vehicle and should use authentication and encryption. D. 235 ¶ 222; D. 192 ¶¶ 175-76.

[10] Some OEMs do not have a secure gateway, D. 220 at 129 (providing one example of vehicle make that does not), while others do. Id. at 132, 152 (referencing one example of a vehicle make that does).

94. Such security protections are technologically feasible to implement (e.g., wireless systems like Bluetooth and WiFi use encryption and already are utilized by OEMs in some vehicles). D. 235 ¶ 222; D. 192 ¶¶ 177, 190.

95. In a fully telematic system, communication to the target ECU for diagnostics would have to route back to the telematics unit (instead of to the J-1962 in the dongle system) when communications initiate from the telematic module. D. 235 ¶ 226; D. 192 ¶ 192.

96. Secure Vehicle Interface ("SVI") is a potential standardized method for securely communicating mechanical data that OEMs could implement with either of the platforms discussed above to achieve standardization as required by Section 3. D. 235 ¶ 233; D. 192 ¶ 200; D. 161-4 ¶¶ 7, 46-54.

97. SVI is a potential method as it has not yet been evaluated or deployed in any wide-scale fashion. D. 219 at 268; see id. at 79.

98. SVI technical standards do not prescribe the specific hardware or software to be used provided that it is capable of meeting these standards. D. 235 ¶ 234; D. 161-4 ¶ 65.

99. The parties' experts, back in June 2021, agreed that such fully telematic systems would take the most time to develop. D. 221 at 52-54, 85-89.

IV. CONCLUSIONS OF LAW

The Attorney General asserts that AAI's preemption claims, Counts I and II, under the MVSA and the CAA, respectively, fail for lack of associational standing and because there is no conflict between the Data Access Law and federal law. For the reasons set forth below, the Court concludes that AAI lacks associational standing to challenge the Data Access Law on behalf of its member automobile manufacturers and that, even assuming *arguendo* that it had such standing, neither the MVSA nor the CAA preempts the Data Access Law.

A. Standing

1. "If a party lacks standing to bring a matter before the court, the court lacks jurisdiction to decide the merits of the underlying case." United States v. AVX Corp., 962 F.2d 108, 113 (1st Cir. 1992); see Cowels v. Fed. Bureau of Investigation, 327 F. Supp. 3d 242, 248 (D. Mass. 2018).

2. "The inquiry into standing seeks to determine 'whether the litigant is entitled to have the court decide the merits of the dispute or of particular issues.'" AVX Corp., 962 F.2d at 113 (quoting Warth v. Seldin, 422 U.S. 490, 498 (1975)).

3. "'The party invoking federal jurisdiction bears the burden of establishing' that it has standing." Massachusetts v. United States Dep't of Health & Hum. Servs., 923 F.3d 209, 221 (1st Cir. 2019) (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 561 (1992)).

4. "[I]n a case like this that proceeds to trial, the specific facts set forth by the plaintiff to support standing 'must be supported adequately by the evidence adduced at trial.'" TransUnion LLC v. Ramirez, 594 U.S. 413, 431 (2021) (quoting Lujan, 504 U.S. at 561).

5. In addition, plaintiffs "must demonstrate standing for each claim that they press and for each form of relief that they seek." Webb v. Injured Workers Pharmacy, LLC, 72 F.4th 365, 372 (1st Cir. 2023) (quoting TransUnion, 594 U.S. at 431).

i. *Associational Standing*

6. AAI does not claim that it has suffered or will suffer any injury from the enforcement of the Data Access Law. Instead, AAI has brought this lawsuit on behalf of its members and asserts their alleged injuries as its basis for standing. D. 235 ¶ 1.

7. Accordingly, AAI has standing for this suit only if it has met the standard for associational standing.

8. "An association has standing to bring suit on behalf of its individual members when: '(a) its members would otherwise have standing to sue in their own right; (b) the interests it seeks to protect are germane to the organization's purpose; and (c) neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit.'" Bos. Parent Coal. for Acad. Excellence Corp. v. Sch. Comm. for City of Bos., 89 F.4th 46, 55 (1st Cir. 2023) (quoting Coll. of Dental Surgeons of P.R. v. Conn. Gen. Life Ins. Co., 585 F.3d 33, 40 (1st Cir. 2009)). Only the third prong of the associational standing test is at issue here.

9. "[J]ust because a claim may require proof specific to individual members of an association does not mean the members are required to participate *as parties* in the lawsuit." Pharm. Care Mgmt. Ass'n v. Rowe, 429 F.3d 294, 306 (1st Cir. 2005) (emphasis in original) (quoting Playboy Enters., Inc. v. Pub. Serv. Comm'n of P.R., 906 F.2d 25, 35 (1st Cir. 1990)); Gathers v. 1-800-Flowers.com, Inc., No. 17-cv-10273-IT, 2018 WL 839381, at *4 (D. Mass. Feb. 12, 2018) (same). But "if adjudicating the merits of an association's claim requires the court to engage in a 'fact-intensive-individual inquiry,'" then "representational standing is inappropriate." New Hampshire Motor Transp. Ass'n v. Rowe, 448 F.3d 66, 72 (1st Cir. 2006) (quoting Pharm. Care Mgmt. Ass'n, 429 F.3d at 314).

10. "We therefore turn to whether [AAI's] preemption claim[s] require[] a sufficiently fact-intensive inquiry to preclude representational standing." Id.

B. Preemption

11. "The Supremacy Clause provides that federal law 'shall be the supreme Law of the Land.'" Consumer Data Indus. Ass'n v. Frey, 26 F.4th 1, 5 (1st Cir. 2022) (quoting U.S. Const. art. VI, cl. 2). "This Clause gives Congress 'the power to preempt state law.'" Id. (quoting Capron v. Off. of Att'y Gen. of Mass., 944 F.3d 9, 21 (1st Cir. 2019)).

12. Both Counts I and II are facial, pre-enforcement challenges to the Data Access Law.

13. Such challenges are disfavored because they are often based on speculation, run contrary to principles of judicial restraint and subvert the democratic process. Wash. State Grange v. Wash. State Republican Party, 552 U.S. 442, 450-51 (2008).

14. For a facial preemption challenge, AAI bears the burden of showing that "no set of circumstances exists under which the [statute] would be valid." NCTA—The Internet & Television Ass'n v. Frey, 7 F.4th 1, 17 (1st Cir. 2021) (internal quotation marks and citation omitted).

15. "There are three types of preemption: conflict, express, and field." Pub. Int. Legal Found., Inc. v. Bellows, 92 F.4th 36, 52 (1st Cir. 2024) (citing New Jersey Thoroughbred Horsemen's Ass'n v. Nat'l Collegiate Athletic Ass'n, 584 U.S. 453, 477-79 (2018)).

16. "Conflict preemption takes place when state law imposes a duty that is 'inconsistent – *i.e.*, in conflict – with federal law.'" Consumer Data Indus. Ass'n, 26 F.4th at 5 (quoting New Jersey Thoroughbred Horsemen's Ass'n, 584 U.S. at 478).

17. This matter concerns conflict preemption, "which itself comes in two varieties: obstacle preemption and impossibility preemption." Capron, 944 F.3d at 21; see Geier v. Am. Honda Motor Co., Inc., 529 U.S. 861, 873, 881 (2000); Town of Acton v. W.R. Grace & Co., No. 13-cv-12376-DPW, 2014 WL 7721850, at *9 (D. Mass. Sept. 22, 2014).

18. "Obstacle preemption is implicated when 'the challenged state law "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress."'" Maine Forest Prods. Council v. Cormier, 51 F.4th 1, 6 (1st Cir. 2022) (quoting Arizona v. United States, 567 U.S. 387, 399 (2012)). "What is a sufficient obstacle is a matter of judgment, to be informed by examining the federal statute as a whole and identifying its purpose and intended effects." Id. (quoting Crosby v. Nat'l Foreign Trade Council, 530 U.S. 363, 373 (2000)). Importantly,

analyzing such implied preemption "does not justify a 'freewheeling judicial inquiry into whether a state statute is in tension with federal objectives'; such an endeavor 'would undercut the principle that it is Congress rather than the courts that pre-empts state law.'" Chamber of Com. of U.S. v. Whiting, 563 U.S. 582, 607 (2011) (quoting Gade v. Nat'l Solid Wastes Mgmt. Ass'n, 505 U.S. 88, 111 (1992)).

19. Also "[f]ederal law impliedly preempts state law 'where it is "impossible for a private party to comply with both state and federal requirements."'" In re Celexa & Lexapro Mktg. & Sales Pracs. Litig., 779 F.3d 34, 40 (1st Cir. 2015) (quoting Mut. Pharm. Co. v. Bartlett, 570 U.S. 472, 480 (2013)). "The question for 'impossibility' is whether the private party could independently do under federal law what state law requires of it." Gustavsen v. Alcon Lab'ys, Inc., 272 F. Supp. 3d 241, 246 (D. Mass. 2017) (quoting PLIVA, Inc. v. Mensing, 564 U.S. 604, 620 (2011)). "If a party 'cannot satisfy its . . . duties' under a state law 'without the Federal Government's special permission and assistance, which is dependent on the exercise of judgment by the federal agency, that party cannot independently satisfy those state duties for pre-emption purposes,' and the state law is preempted." Id. (quoting PLIVA, Inc., 564 U.S. at 623-24).

20. The First Circuit has repeatedly cautioned that "[p]reemption is strong medicine, not casually to be dispensed." Grant's Dairy--Maine, LLC v. Comm'r of Maine Dep't of Agric., Food & Rural Res., 232 F.3d 8, 18 (1st Cir. 2000); Brown v. United Airlines, Inc., 720 F.3d 60, 71 (1st Cir. 2013) (same). Indeed, "a high threshold must be met if a state law is to be preempted for conflicting with the purposes of a federal Act," Whiting, 563 U.S. at 607 (internal quotation marks and citation omitted), and "[t]he Supreme Court has instructed that preemption based on impossibility is a 'demanding defense,'" In re Zofran (Ondansetron) Prods. Liab. Litig., 57 F.4th 327, 336 (1st Cir. 2023) (quoting Wyeth v. Levine, 555 U.S. 555, 573 (2009)).

21. "In all [preemption] cases, . . . we 'start with the assumption that the historic police powers of the States were not to be superseded by the Federal Act unless that was the clear and manifest purpose of Congress.'" Pub. Int. Legal Found., Inc., 92 F.4th at 51 (alterations in original) (quoting Medtronic, Inc. v. Lohr, 518 U.S. 470, 485 (1996)).

22. "And whether or not the presumption against preemption applies, the burden of proving preemption lies with the part[y] asserting it (here, the plaintiff[])." See Maine Forest Prods. Council, 51 F.4th at 6.

23. AAI asserts that the Data Access Law is preempted because "[c]ompliance with the Data Access Law would require OEMs to abandon existing cybersecurity and emissions controls that protect core vehicle functions—directly controverting the requirements, purposes, and objectives of the [MVSA] and the [CAA]." D. 340 at 9. Both Counts I and II are addressed in turn below, but since both claims involve statutory construction, the Court begins there.

C. Construction of the Data Access Law

24. At the outset, the Court notes that it has considered the parties' respective interpretations of the Data Access Law. See generally D. 235 ¶¶ 29-57; D. 236 ¶¶ 40-90; D. 290, 292, 293.

25. Ultimately, however, "the 'duty of statutory interpretation is for the courts.'" Case of Moss, 451 Mass. 704, 709 (2008) (quoting In re Slater's Case, 55 Mass. App. Ct. 326, 330 (2002)).

26. "In every question of statutory interpretation, we begin our analysis with the plain language of the statute." Commonwealth v. Escobar, 490 Mass. 488, 493 (2022); Makis M. v. Commonwealth, 494 Mass. 23, 30 (2024) (noting that "[i]n the absence of statutory definitions, we read the words of a statute to have their 'plain and ordinary meaning'") (quoting Matter of E.C., 479 Mass. 113, 118 (2018)).

27. "If we determine that statutory language is unknowably ambiguous or 'faulty or lacks precision, it is our duty to give the statute a reasonable construction.'" Makis M., 494 Mass. at 30-31 (quoting Com. v. Keefner, 461 Mass. 507, 511 (2012)). "[W]e must construe the statute 'in connection with the cause of its enactment, the mischief or imperfection to be remedied and the main object to be accomplished, to the end that the purpose of its framers may be effectuated.'" Capone v. Zoning Bd. of Appeals of Fitchburg, 389 Mass. 617, 622-23 (1983) (quoting Indus. Fin. Corp. v. State Tax Comm'n, 367 Mass. 360, 364 (1975)); Keefner, 461 Mass. at 511 (same).

28. With these legal principles in mind, the Court construes the contested provisions of the Data Access Law only as necessary and to the extent below.[11]

29. As to the added definition of "mechanical data" in Section 1 of Mass. Gen. L. c. 93K, this term is defined as "any vehicle-specific data, including telematics system data, generated, stored in or transmitted by a motor vehicle used for or otherwise related to the diagnosis, repair or maintenance of the vehicle."

[11] To the extent AAI contends that the "key revisions to several specific aspects" of the Data Access Law that were made to the Maine ballot initiative reflect "an implicit concession that safe compliance with the Massachusetts law is not possible," D. 335 at 3, the Court disagrees. That the same proponent may have been involved in the initiatives both in Massachusetts and in Maine is not persuasive or dispositive of the construction that the Court must do here, given the language adopted in the Data Access Law, now codified in Mass. Gen. L. c. 93K. Cf. State of R.I. v. Narragansett Indian Tribe, 19 F.3d 685, 699 (1st Cir. 1994) (noting that "statements by individual legislators should not be given controlling effect; rather, such statements are to be respected only to the extent that they are consistent with the statutory language" at issue)(internal quotation marks and citation omitted); Weinberger v. Rossi, 456 U.S. 25, 35 n.15 (1982) (noting that "[t]he contemporaneous remarks of a sponsor of legislation are certainly not controlling in analyzing legislative history"). Moreover, that AAI and the Attorney General of Maine are now in dispute about the alleged unenforceability of the newly enacted Maine Data Law on due process and federal preemption grounds, see Alliance for Auto. Innovation v. Att'y General of Maine, No. 25-cv-00041-LEW, also suggests that such reliance would be unwise.

30. The last phrase of this definition—"used for or otherwise related to the diagnosis, repair or maintenance of the vehicle"—limits "mechanical data" to data used for or related to same. D. 235 ¶ 38.

31. Data unrelated to diagnostics, maintenance or repair is not within the scope of "mechanical data" under Section 1. D. 235 ¶ 39. "If the statute's language is plain, 'the sole function of the courts—at least where the disposition required by the text is not absurd—is to enforce it according to its terms.'" In re Rudler, 576 F.3d 37, 44 (1st Cir. 2009) (quoting Lamie v. U.S. Tr., 540 U.S. 526, 534 (2004)). Here, even as "none of the words of a statute is to be regarded as superfluous," Com. v. Woods Hole, Martha's Vineyard & Nantucket S. S. Auth., 352 Mass. 617, 618 (1967) (quoting Bolster v. Comm'r of Corps. & Tax'n, 319 Mass. 81, 84-85 (1946)), the Court concludes that the plain language of the statute does not encompass data unrelated to diagnostics, maintenance or repair.[12]

32. This construction does not conflict with the prior version of Mass. Gen. L. c. 93K, as AAI suggests, where the prior version did not include a definition of "mechanical data" and excluded telematics services except as necessary to diagnose and repair vehicles. Mass. Gen. L. c. 93K, §§ 1, 2(f) (Nov. 26, 2013) (superseded). The current definition includes telematics and makes clear that it covers data used for or otherwise related to the "diagnosis, repair or maintenance of the vehicle." Mass. Gen. L. c. 93K, § 1.

33. This construction is consistent with other provisions of Mass. Gen. L. c. 93K, which make clear that it does not require independent repair shops to receive access to non-diagnostic and

[12] Contrary to AAI's suggestion otherwise, D. 364 at 53, Lowe's agreement that the inclusion of "otherwise related to" was "sort of a catch-all so that there would not be a narrow interpretation of what is related to diagnosis, repair and maintenance," D. 220 at 24; see id. at 64, is not contrary to this construction.

repair information. D. 235 ¶ 40; Mass. Gen. L. c. 93K, § 5 (providing that "[n]othing in this chapter shall be construed to require manufacturers or dealers to provide an owner or independent repair facility access to non-diagnostic and repair information provided by a manufacturer to a dealer or by a dealer to a manufacturer pursuant to the terms of a franchise agreement").

34. As to Section 2, the phrase "access to vehicle networks and their on-board diagnostic systems" refers not to access for any purpose whatsoever, but rather to access to obtain data related to the purposes of diagnosis, repair and maintenance. D. 235 ¶¶ 43-44, 62.

35. Regardless of the parties' dispute about whether the term "authorization" includes the concept of authentication, see D. 236 ¶¶ 60-62; D. 235 ¶¶ 45-47, and contrary to AAI's contention, Section 2 does not bar any authorization by the manufacturer directly or indirectly, D. 236 ¶ 56, but instead bars same "unless the authorization system for access to vehicle networks and their on-board diagnostic systems is standardized across all makes and models sold in the Commonwealth and is administered by an entity unaffiliated with a manufacturer." Mass. Gen. L. c. 93K, § 2(d)(1).

36. Moreover, the language "an entity unaffiliated with a manufacturer" means an entity not affiliated with an OEM but does not bar any role by an OEM in an authorization system. D. 235 ¶ 61; cf. D. 236 ¶ 66.

37. As to Section 3, that beginning in model year 2022 and thereafter, "a manufacturer of motor vehicles sold in the Commonwealth . . . that utilizes a telematics system shall be required to equip such vehicles with an inter-operable, standardized and open access platform across all of the manufacturer's makes and models," Mass. Gen. L. c. 93K, § 2(f), means that the OEMs cannot act as a gatekeeper to the platform and its mechanical data. D. 235 ¶ 69.

38. Specifically, "platform" refers to vehicle architecture and associated software and features. Id. ¶ 51.

39. The term "interoperable" refers to a standard way to connect and communicate with the vehicle that can be used regardless of the manufacturer. Id. ¶ 52.

40. The term "standardized" means to follow a common and well documented method to perform the necessary actions such that there is a common, agreed-upon way of communicating. Id. ¶ 53; D. 236 ¶ 77.

41. "Open access" means to have a non-gated means of access to the mechanical data for the owner without the OEM as a gatekeeper, D. 235 ¶ 54, but it does not mean "open access" to others other than the owner, independent repair shop or dealer licensed to do repairs, particularly in light of the language that follows in Section 3. Mass. Gen. L. c. 93K, § 2(f) (providing further that "[s]uch [open access] platform shall be directly accessible by the owner of the vehicle through a mobile-based application and, upon the authorization of the vehicle owner, all mechanical data shall be directly accessible by an independent repair facility or a class 1 dealer . . . limited to the time to complete the repair or for a period of time agreed to by the vehicle owner for the purposes of maintaining, diagnosing and repairing the motor vehicle").

42. Similarly, "directly accessible" means that the vehicle owner will not need to go through the OEM to perform diagnosis, maintenance and repairs. D. 235 ¶ 55.

43. None of this construction is at odds with the plain language of the statute or the purposes of the Data Access Law.

44. Putting aside any "great weight" to the Attorney General's interpretation of a state law,[13] McGuire v. Reilly, 386 F.3d 45, 55, 64 (1st Cir. 2004), as AAI urges this Court to do, D. 236

[13] In 2024, the Supreme Court in Loper Bright Enterprises v. Raimondo, 603 U.S. 369, 412-13 (2024) overruled the Chevron doctrine. However, "[a]s a federal case decided under the federal [Administrative Procedure Act] Loper has no direct application here." Associated Gen. Contractors of Cal., Inc. v. Dep't of Indus. Rels., No. C098009, 2025 WL 261942, at *8 n.5 (Cal. Ct. App. Jan. 22, 2025) (examining regulations issued to implement a prevailing state wage law).

¶¶ 41-44, in adopting this construction, the Court concludes that this is reasonable construction, informed by canons of interpretation and that even where "[t]here is a basic uncertainty about what the law means and how it will be enforced," "without the benefit of a definitive interpretation from the state courts, it would be inappropriate to assume [the state law] will be construed in a way that creates a conflict with federal law." See Arizona, 567 U.S. at 415; see also Bates v. Dow Agrosciences LLC, 544 U.S. 431, 449 (2005) (concluding that even if party's alternative reading of the text "were just as plausible as [the Court's] reading of that text," the Court "would nevertheless have a duty to accept the reading that disfavors pre-emption").[14]

45. In fact, the experts for both parties engaged in a "hot tub" discussion in which they acknowledged that the construction of the Data Access Law mattered as to their opinions. D. 221. Notably, over the course of the hot tub, the experts for AAI indicated that under the narrower construction of the Data Access Law advanced by the Attorney General, they might take a different view of the feasibility of implementing the statute in a way that is consistent with federal law. Bort, for example, explained that "[s]o much of [the] disagreement really comes down to what are we trying to answer." Id. at 48. He suggested that if the Data Access Law were construed more narrowly and not in the "unbounded" way in which he had been interpreting it, "then that's a

---

This Court further takes note, however, that "[a]lthough Loper did not expressly overrule Auer [v. Robbins, 519 U.S. 452 (1997)] and Kisor [v. Wilkie, 588 U.S. 558 (2019)], its reasoning is arguably irreconcilable with Auer deference." Humboldt All. for Responsible Plan. v. Cal. Coastal Comm'n, 328 Cal. Rptr. 3d 188, 197 (Cal. App. 1st Dist. 2024) (citing Auer v. Robbins, 519 U.S. 452 (1997) (holding that an agency's reading of its own ambiguous regulation may receive substantial deference); Kisor v. Wilkie, 588 U.S. 558 (2019) (declining to overrule Auer deference to agencies' reasonable readings of genuinely ambiguous regulations)), as modified (Nov. 25, 2024), reh'g denied (Jan. 7, 2025). In any event, the Court here does not give any deference to the Attorney General's construction of the Data Access Law.

[14] Given this construction, the Court need not reach the parties' arguments about severability. D. 235 ¶¶ 112-16; D. 236 ¶¶ 137-43.

different scope, and I wouldn't have an issue with that." Id. at 79. Garrie, too, testified that under an alternate reading of the statute, "it seems a lot more feasible." Id. at 58; see D. 219 at 189.[15]

46. Given this construction, the Court turns to AAI's conflict preemption claims.

D. Count I: National Traffic and Motor Vehicle Safety Act

47. Count I of the complaint seeks a declaration that the Data Access Law is unenforceable because it is preempted by the MVSA and federal motor vehicle safety standards ("FMVSS") promulgated by the National Highway Traffic Safety Administration ("NHTSA").

48. Specifically, AAI challenges Section 2 of the Data Access Law, which requires either (i) that "motor vehicle owners' and independent repair facilities' access to vehicle on-board diagnostic systems . . . be standardized and not require any authorization by the manufacturer" or (ii) that "the authorization system for access to vehicle networks and their on-board diagnostic systems [be] standardized across all makes and models sold in the Commonwealth and [be] administered by an entity unaffiliated with a manufacturer." Mass. Gen. L. c. 93K, § 2(d)(1). AAI also challenges Section 3 of the Data Access Law, which requires manufacturers to equip vehicles beginning in model year 2022 with an "inter-operable, standardized and open access platform." Mass. Gen. L. c. 93K, § 2(f).

49. NHTSA has the authority to issue and enforce FMVSS for vehicles and equipment and to issue recalls to address and remediate safety-related defects in vehicles. D. 236 ¶ 102.

[15] AAI's other witnesses also relied upon a broader view of the Data Access Law than construed by the Court. See, e.g., D. 219 at 119 (opining by Baltes that "open access" means access "for everyone with unrestricted use with no authorization required by the manufacturer"); id. at 54-55 (offering by Tierney that law requires access to all networks simultaneously); id. at 125 (testifying by Chernoby that "open access" would be for anybody and would be a "very, very broad audience").

50. Even where NHTSA does not order a recall, it can engage manufacturers to undertake their own voluntary recall, D. 198 ¶ 33; D. 199 ¶ 20, or the issuance of a safety recall report as Fiat has done on one occasion in 2015 regarding a vulnerability in the telematics system. D. 199 ¶¶ 29-34.

51. That 2015 voluntary recall by Fiat was not mandated by NHTSA and did not involve a determination that the vulnerability constituted a safety defect. D. 219 at 133.

52. AAI contends that the requirements of the Data Access Law conflict with the "make inoperative" provision of the MVSA, which prohibits OEMs from "knowingly mak[ing] inoperative any part of a device or element of design installed on or in a motor vehicle or motor vehicle equipment in compliance with an applicable motor vehicle safety standard." 49 U.S.C. § 30122(b). AAI further asserts that the Data Access Law is preempted by various FMVSS that concern acceleration, braking, steering and air bag systems because OEMs "have installed a variety of cybersecurity protections around regulated vehicle functions" and "[y]et the Data Access Law requires motor vehicle manufacturers to remove cybersecurity protections." D. 340 at 10 (citing 49 C.F.R. § 571.124 (acceleration control devices); id. § 571.126 (electronic stability control, including steering and anti-lock braking systems); id. § 571.135 (light-vehicle braking systems); id. § 571.208 (occupant crash protection, including air bags)).

i. *Obstacle Preemption*

53. AAI has not met its burden to prove that the Data Access Law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress with respect to the MVSA.

54. There is no "significant objective" of the MVSA or the FMVSS that is thwarted by the Data Access Law. Williamson v. Mazda Motor of Am., Inc., 562 U.S. 323, 330 (2011).

55. No provision in the MVSA directly addresses motor vehicle cybersecurity or access to motor vehicle diagnostic data, nor do any of the FMVSS that AAI cites, see FMVSS 124, 126, 135, 208, 42 C.F.R. §§ 571.124, 571.126, 571.135, 571.208; D. 197 ¶ 22; D. 199 ¶ 17, discuss cybersecurity protections, much less adopt a federal cybersecurity objective that conflicts with the Data Access Law. D. 235 ¶ 77.

56. That NHTSA has the general authority to address vehicle safety risks through recalls, 49 U.S.C. §§ 30118-30122, does not support a conclusion that a "significant objective" of the federal statutory scheme is thwarted by the Data Access Law.

57. Even if there was a past, voluntary recall by Fiat in 2015, D. 219 at 132, on the present record, it is speculative if there would be any recall, voluntary or mandated, by NHTSA relating to compliance with the Data Access Law.

58. Even for obstacle preemption, it is not enough for AAI to point to the general purpose of NHTSA and MVSA in prompting vehicle safety to say that a "significant objective" of the federal statutory scheme is thwarted by the Data Access Law.

59. That is, in undertaking a preemption analysis, "it is necessary to look beyond general expressions of 'national policy' to specific federal statutes with which the state law is claimed to conflict." Commonwealth Edison Co. v. Montana, 453 U.S. 609, 634 (1981) (citation omitted). "Viewed at a high level of generality, every provision in a statute will relate to its overarching purpose. The real question is whether the alleged statutory violation is among the concrete harms Congress enacted the law to remedy." Thorne v. Pep Boys Manny Moe & Jack Inc., 980 F.3d 879, 892 (3d Cir. 2020). That is, "[t]o succeed, [AAI] 'must show that applying the state law would do "major damage" to clear and substantial federal interests.'" See McHenry

Cnty. v. Kwame Raoul, 44 F.4th 581, 591 (7th Cir. 2022) (quoting C.Y. Wholesale, Inc. v. Holcomb, 965 F.3d 541, 547 (7th Cir. 2020)).

60. That AAI has not sustained its burden here as to preemption also is supported by the MVSA's saving clause, 49 U.S.C. § 30103(d) (noting that the statute "do[es] not establish or affect a warranty obligation under a law of the United States or a State" and that remedies under the statute are "in addition to other rights and remedies under other laws of the United States or a State"), which applies to the recall provisions and other rights and remedies under the law.

61. The Data Access Law does not require removing or disabling safety equipment or features installed to comply with an FMVSS where, for instance, none of the FMVSS that govern acceleration, braking, steering and airbag systems, D. 236 ¶¶ 120-24, mention cybersecurity protections.

62. As is clear from the record, vehicle cybersecurity is not covered by any existing FMVSS. D. 235 ¶ 77 (citing Nat'l Highway Traffic Safety Admin., Cybersecurity Best Practices for Modern Vehicles (2016) ("2016 NHTSA Guidance") at 5 (noting that "vehicle cybersecurity . . . is not covered by an existing [FMVSS] at this time"); D. 198 ¶ 32; D. 199 ¶ 24.

63. The stated purpose of the 2016 NHTSA guidance was to describe the agency's "non-binding guidance to the automotive industry for improving motor vehicle cybersecurity." D. 235 ¶ 80; see D. 236 ¶ 107.

64. To the extent that AAI relies upon the 2016 NHTSA Guidance, that document is non-binding guidance and does not provide a basis for obstacle preemption, as AAI has acknowledged. D. 236 ¶ 109 (noting that "agency guidance does not itself have preemptive effect"); see Holk v. Snapple Beverage Corp., 575 F.3d 329, 339-42 (3d Cir. 2009) (concluding that agency's policy statement is not entitled to preemptive effect even if the agency enforced it in

"isolated instances"); Good v. Altria, 501 F.3d 29, 51 (1st Cir. 2007) (holding that "[l]imiting the preemptive power of federal agencies to exercises of formal rulemaking authority" ensures that states will benefit from those protections "before suffering the displacement of their laws"); Koenig v. Boulder Brands, Inc., 995 F. Supp. 2d 274, 285 (S.D.N.Y. 2014) (concluding that "[a]s it is non-binding guidance, the FDA's Compliance Policy Guide 'is not entitled to preemptive effect'") (internal citation omitted); see also 49 U.S.C. § 30111(f)(1) (observing that "[n]o guidelines issued by the Secretary with respect to motor vehicle safety shall confer any rights on any person, State or locality nor shall operate to bind the Secretary or any person to the approach recommended in such guidance").

65. Although AAI urges the Court to consider the agency's views as "highly probative in determining preemption," D. 236 ¶ 109 (and cases cited), more recent NHTSA guidance recommends that cybersecurity "should not become a reason to justify limiting serviceability" by independent repair shops. D. 235 ¶ 81; Nat'l Highway Traffic Safety Admin., Cybersecurity Best Practices for the Safety of Modern Vehicles (2022) at 12, https://www.nhtsa/gov/sites/nhtsa.gov/files/2002-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf (last visited Feb. 10, 2025).

66. Even in its more recent communications filed in this case, the June 2023 NHTSA Letter and the August 2023 NHTSA letter, NHTSA does not promulgate or cite standards for data access or cybersecurity. D. 346-1; D. 351-1. The first letter, addressed to OEMs, expressed concerns about the breadth of any "open access" to a motor vehicle's telematics, D. 346-1, which is a construction of the Data Access Law that this Court has rejected above. Moreover, in the subsequent August 2023 NHTSA letter, also filed publicly in case, D. 351-1, NHTSA noted that it had worked with the Attorney General's office "to identify a way that the [Data Access Law] may

be successfully implemented—promoting consumers' ability to choose independent or do-it-yourself repairs—without compromising safety." Id. at 1 (discussing "short-range wireless protocols" for access to mechanical data for vehicle owners and independent repair shops); see D. 352-1 (responding to the August 2023 NHTSA Letter, the Attorney General "confirm[s] NHTSA's understanding that a platform that provides the required features, capabilities, and access using a short-range wireless protocol such as Bluetooth is one approach that a vehicle manufacturer might use to achieve compliance with the Data Access Law").

67. Neither NHTSA's initial expression of concern nor the absence of development of this protocol at this time, see D. 351-1 at 2 (noting that this "compliance option . . . is not immediately available, and that vehicle manufacturers may require a reasonable period of time to securely develop, test, and implement this technology"), support AAI's burden to show that compliance with the Data Access would thwart the objectives and purposes of the MVSA.

68. Case law is instructive on this point as well. In Sprietsma v. Mercury Marine, a Div. of Brunswick Corp., 537 U.S. 51 (2002), the Supreme Court held that "a Coast Guard decision not to regulate a particular aspect of boating safety is fully consistent with an intent to preserve state regulatory authority pending the adoption of specific federal standards." Id. at 65. The decision of NHTSA not to regulate vehicle cybersecurity is similarly consistent with an intent to preserve state regulatory authority. See id.; Durham v. Cnty. of Maui, 696 F. Supp. 2d 1150, 1159 (D. Haw. 2010) (noting "FMVSS 208 does not conflict with Plaintiffs' side-impact airbag claims because FMVSS 208 contains no side-impact airbag requirements, much less conflicting ones").

69. "[A] high threshold must be met if a state law is to be preempted for conflicting with the purposes of a federal Act," Whiting, 563 U.S. at 607 (quoting another source), and AAI has not

met that high threshold of demonstrating that any provision of the Data Access Law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress.

ii. *Impossibility Preemption*

70. Nor has AAI established that complying with both the Data Access Law and the MVSA and FMVSS would be a "physical impossibility." Arizona, 567 U.S. at 399 (noting that for this form of conflict preemption, plaintiff must show that compliance with both federal and state law is a "physical impossibility").

71. As discussed, vehicle cybersecurity "is not covered by an existing [FMVSS]," D. 235 ¶ 77, and where "there is simply no federal standard for a private party to comply with," "it is not impossible for petitioners to comply with both federal and state law," Freightliner Corp. v. Myrick, 514 U.S. 280, 289 (1995).

72. To the extent that AAI relies upon the "make inoperative" provision of the MVSA, 49 U.S.C. § 30122(b) (providing that manufacturers and others "may not knowingly make inoperative any part of a device or element of design installed on or in a motor vehicle or motor vehicle equipment in compliance with an applicable motor vehicle safety standard"), such argument also fails as addressed above.

73. As also discussed above, neither the MVSA nor the FMVSS address or regulate cybersecurity or access to vehicle data.

74. Thus, it is not a physical impossibility for OEMs to comply with such federal laws and the Data Access Law since there are no applicable federal standards for same.

75. As to Section 2, AAI's contention that the present non-existence of any standardized authorization system through a third party prevents its compliance with the Data Access Law, D. 236 ¶¶ 65, 73, 114, does not support its impossibility preemption claim which is focused on the

impossibility of complying both with the Data Access Law and federal law. Gustavsen, 272 F. Supp. 3d at 246.

76. Much of AAI's affidavits and testimony focused on the impossibility or difficulty of complying with the Data Access Law, see, e.g., D. 197 ¶ 12 (attesting by Tierney that "GM's multi-year product development process makes it impossible for GM to develop and implement the considerable changes to vehicle architecture required by the Data [Access] Law"), as opposed to the impossibility of complying with it and federal law.

77. The former focus might be a defense to a later enforcement action under the Data Access Law, see Le Fort Enters., Inc. v. Lantern 18, LLC, 491 Mass. 144, 151 (2023) (observing that Massachusetts courts "have 'long recognized and applied the doctrine of impossibility as a defense to an action for breach of contract'" (quoting Chase Precast Corp. v. John J. Paonessa Co., 409 Mass. 371, 373 (1991))); Fortin v. Comm'r of Mass. Dep't of Pub. Welfare, 692 F.2d 790, 796 (1st Cir. 1982) (noting that "impossibility would be a defense to contempt"); In re Care & Prot. of Summons, 437 Mass. 224, 237 (2002) (observing that "[n]oncompliance with a judge's valid order may be excused where it becomes impossible"); see D. 364 at 24 (acknowledging same by counsel for the Attorney General), but not as a basis for preemption claims in Count I and Count II.

78. Indeed, as noted, "[t]he question for 'impossibility' is whether the private party could independently do under federal law what state law requires of it." Gustavsen v. Alcon Lab'ys, Inc., 272 F. Supp. 3d at 246 (quoting PLIVA, 564 U.S. at 620). A party can "independently satisfy [its] state duties for pre-emption purposes" when satisfaction of those state duties does not require "the Federal Government's special permission and assistance." See PLIVA, Inc., 564 U.S. at 623-24. Here, the issues that AAI's member automobile manufacturers may face, if any, in complying with the MVSA do not stem from conflicting federal regulations, nor would complying with the

state statute require the federal government's special permission or assistance or "the exercise of judgment by [a] federal agency." See Gustavsen, 272 F. Supp. 3d at 246.

79. Although, setting aside whether the OEMs could comply with the Data Access Law by "walk[ing] off the field" in some manner, all four experts agreed at the outset of the hot tub discussion at trial that "the kinds of platforms that are talked about" in connection with the statute could not immediately be provided by the OEMs. D. 221 at 41 (Smith (answering "[d]efinitely not right away")); id. at 42 (Romansky (thinking that "the elements of a solution are available, but they're not assembled, and that has not been proven to all work together" and that it would "take some engineering work, problem-solving to bring them together and make it work")); id. (Bort ("agree[ing] with both the other experts" and adding that "I don't think we can do that right now")); id. (Garrie ("agree[ing] with my colleagues")). That agreement, however, was as matter of building vehicle architecture and technology, not as a matter of the impossibility of complying with both the Data Access Law and federal law.

80. Whether such system has been built yet, D. 364 at 9-10, the experts' agreement that compliance with the Data Access Law is possible does not support AAI's burden to show that compliance with that law and the MVSA is impossible.

81. As to Section 3, AAI has asserted "that it is a 'practical impossibility' for manufacturers to disable telematics only for vehicles sold in the Commonwealth," D. 236 ¶ 86, and offered evidence that at least some auto manufacturers may not be able to do so, see id. ¶ 129. Following trial, however, the parties jointly stipulated that in June 2021, a different auto manufacturer and AAI member (not participating in discovery here), Subaru, implemented a policy of not making its telematics system available to Massachusetts residents who purchase or lease model year 2022 vehicles. D. 262 ¶ 3. The parties further stipulated that "Subaru vehicles that are not enrolled in

the [telematics] system are safe," and that such vehicles "comply with all applicable Federal Motor Vehicle Safety Standards." Id. ¶ 6.

82. Whatever the stage of development of other means of complying with Section 3, D. 236 ¶ 81, disabling telematics is at least one method of complying with Section 3 (or at least not being subject to Section 3) for the reasons discussed above. D. 192 ¶¶ 78-87; D. 219 at 252 (acknowledging by Garrie that if the third-party entity envisioned by Section 3 existed and "all of the other pieces" were in place, it would be possible to comply with the Data Access Law).

83. This information and post-trial stipulation about Subaru show that GM and Fiat's approach to cybersecurity and data access is not necessarily representative of OEMs in general.

84. Accordingly, AAI has not met its burden of demonstrating that compliance with the Data Law and the MVSA is an impossibility.

85. Moreover, the analysis above illustrates that "member circumstances differ" with respect to OEMs' ability to comply with the Data Access Law. Pharm. Care Mgmt. Ass'n, 429 F.3d at 314 (Boudin, J., concurring).

E. Count II: Clean Air Act

86. Count II of the complaint seeks a declaration that the Data Access Law is unenforceable because it is preempted by the CAA.

87. Through the CAA, Congress has established a comprehensive statutory scheme to control air pollution from all sources in the United States. D. 236 ¶ 126.

88. As part of this scheme, the CAA imposes stringent vehicle emission requirements on manufacturers including warrantying the emission control system of their vehicles for their "useful life" (i.e., ten years or 100,000 miles). D. 236 ¶ 129 (citing 42 U.S.C. §§ 7521(d), 7541(a)(1)); D. 196 ¶ 29 (citing 42 U.S.C. § 7521).

89. If a manufacturer does not comply with the CAA emissions limits, the EPA may bring an enforcement action against it. D. 196 ¶ 35.

90. The EPA also has the authority to enforce compliance through recalls. D. 199 ¶ 15.

91. There is no provision of the CAA that precludes compliance with the Data Access Law.

92. Similar to their preemption challenge to the MVSA, AAI relies upon the provision of the CAA that prohibits "any person [from] remov[ing] or render[ing] inoperative any device or element of design installed on or in a motor vehicle or motor vehicle engine in compliance with regulations under this subchapter prior to its sale and delivery to the ultimate purchaser, or for any person knowingly to remove or render inoperative any such device or element of design after such sale and delivery to the ultimate purchaser." 42 U.S.C. § 7522(a)(3)(A); D. 236 ¶ 130.

93. AAI contends that compliance with the Data Access Law would require eliminating or degrading cybersecurity controls that protect against cyber intrusion of emission-related vehicle components. D. 236 ¶ 135.

i. *Obstacle Preemption*

94. Other than the aforementioned provision requiring access to emissions data, there is no other provision of the CAA or its regulations that regulates vehicle cybersecurity or data access controls.

95. Moreover, that provision of the CAA requires that manufacturers "provide promptly to any person engaged in the repairing or servicing of motor vehicles or motor vehicle engines . . . any and all information needed to make use of the emission control diagnostics system prescribed under this subsection and such other information including instructions for making emission related diagnosis and repairs." 42 U.S.C. § 7521(m)(5); see 40 C.F.R. § 86.1808-01(f)(2)(i); 40 C.F.R. § 86.010-38(j)(3)(i).

96. Thus, far from reflecting a purpose of restricting access to emissions-control data, the CAA instead reflects Congress's purpose of making such information available.

97. Moreover, the saving clause of the CAA preserves the right of states "to control, regulate, or restrict the use, operation or movement of registered or licensed motor vehicles." 42 U.S.C. § 7543(d).

98. Accordingly, the Data Access Law—which seeks to provide for more uniform access to vehicles' diagnostics systems—does not stand as an obstacle to the accomplishment of the full purposes and objectives of the CAA.

ii. *Impossibility Preemption*

99. Nor is it impossible to comply with both the Data Access Law and the CAA.

100. AAI contends that the Data Access Law would require manufacturers to remove cybersecurity design elements that help to protect against cyber intrusion of emissions-related vehicle components, and that manufacturers therefore cannot comply with both the Data Access Law and the CAA. D. 236 ¶¶ 134-36.

101. As discussed, AAI stipulated that "[a]s a direct result of Section 3 of the Data Access Law," Subaru decided not to make its telematics system available to Massachusetts residents who purchase or lease model year 2022 vehicles, and that such vehicles are in compliance with the CAA and all applicable regulations promulgated thereunder. D. 262 ¶¶ 3, 6.

F. <u>Returning to the Issue of Associational Standing</u>

102. This part of the record, stipulated by the parties, illustrates that AAI has not satisfied the third prong of associational standing where "member circumstances differ" with respect to compliance with the Data Access Law, <u>Pharm. Care Mgmt. Ass'n</u>, 429 F.3d at 314 (Boudin, J.,

concurring), despite AAI's contention that it would be impossible to do so and also impossible to do so and comply with federal law.

103. Even assuming *arguendo*, however, that AAI had shown associational standing, its preemption claims under Count I and Count II fail.

104. Even while crediting the testimony of the witnesses from GM and Fiat about the difficulty of at least two manufacturers in complying with the Data Access Law, the Court concludes, as a matter of law, that AAI has not met its burden of showing that a significant objective of the MVSA or CAA is thwarted by the Data Access Law or that it has shown an impossibility of complying with the Data Access Law and either of those federal schemes.

105. For the reasons set forth above, the Court concludes that AAI lacks associational standing to assert either of its remaining preemption claims,[16] and that in any event, AAI has not met its burden to prove that either the MVSA or CAA preempts the Data Access Law.[17]

---

[16] At the time the Court dismissed Counts III through VIII, the Court stated that it was doing so for reasons that would be developed in the Memorandum of Decision to be issued regarding the Findings and Conclusions. D. 334. Accordingly, the Court adds this footnote to explain that AAI lacks associational standing as to the previously dismissed Counts. As to Count VII, AAI asserts that the Data Access Law effects both a physical and regulatory taking. Resolution of a Takings Clause claim requires an "essentially ad hoc, factual inquir[y]." Kaiser Aetna v. United States, 444 U.S. 164, 175 (1979). Here, resolving AAI's Takings Clause claim would require engaging in an ad hoc factual inquiry for member OEMs that allege that it will suffer a taking by complying with the Data Access Law. As to this matter, member circumstances also differ. See Pharm. Care Mgmt. Ass'n, 429 F.3d at 314 (Boudin, J., concurring). Accordingly, the Court concludes that AAI lacks associational standing to assert Count VII. As to the other federal preemption claims, Counts III through VI, there would also be a need for member determinations as to the various intellectual property rights at issue in AAI's preemption challenges to the Copyright Act (Count III), the Defend Trade Secrets Act (Count IV), the Computer Fraud and Abuse Act (Count V), and the Digital Millennium Copyright Act (Count VI). Accordingly, the Court concludes that AAI lacks associational standing to bring Counts III through VII (and so much of Count VIII that sought declaratory and injunctive relief for same).

[17] In light of the Court's rulings regarding lack of associational standing and rejection of the remaining federal preemption claims under Counts I and II for the reasons addressed above, the Court does not reach the Attorney General's alternative argument that Counts I and II also fail

V. CONCLUSION

Given these findings of fact and conclusions of law, the Court dismisses Counts I and II (and any remainder of Count VIII that sought injunctive relief for Counts I and II) of the complaint and shall enter judgment for the Attorney General.

So Ordered.

/s Denise J. Casper
U.S. District Judge

because AAI has not identified any right of action that entitles it to pursue such claims of preemption under either the MVSA or the CAA. D. 235 ¶¶ 11 *et seq.* (citing, among other cases, Armstrong v. Exceptional Child Ctr., Inc., 575 U.S. 320, 324 (2015)); D. 342 at 5-6.